UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/672,796 | 09/26/2003 | Andrew Morgan | TRAN-P162 | 9469 |

45590 7590 07/07/2009
TRANSMETA C/O MURABITO, HAO & BARNES LLP
TWO NORTH MARKET STREET
THIRD FLOOR
SAN JOSE, CA 95113

| EXAMINER | |
|---|---|
| PICH, PONNOREAY | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2435 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 07/07/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| | | | |
|---|---|---|---|
| *Office Action Summary* | **Application No.**<br>10/672,796 | **Applicant(s)**<br>MORGAN ET AL. | |
| | **Examiner**<br>PONNOREAY PICH | **Art Unit**<br>2435 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *07 May 2009*.

2a)□ This action is **FINAL**.  2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 18-26* is/are rejected.

7)☒ Claim(s) *16-17* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *6/09*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/7/09 has been entered.

Claims 1-26 are pending.

### ***Response to Amendment and Arguments***

Applicant's amendment and arguments directed at the amended claims were fully considered. Applicant's argument that the prior art of record does not teach the new limitation of "wherein the internal memory is further configured to store data associated with the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein the data is accessible only within the processor" is moot in view of new rejections made below in response to the amendments.

Applicant's argument that the prior art does not teach the limitation of claim 16 as amended was considered and was persuasive. An updated search confirms that the prior art does not teach the combination of limitations as currently recited in claim 16. As indicated below, claim 16 would be allowable if it was rewritten in independent form with all the limitations of any parent claims.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-7, 9-11, 14-15, 18-21, and 25 are rejected under 35 U.S.C. 103(a) as obvious over Easter et al (US 5,563,950) in view of Hashimoto et al (US 6,983,374).

**Claim 1:**

Easter discloses:

1. A digital secret including a secret key (i.e. the DES secret key) used in a key-based cryptographic process, wherein the digital secret is operable to be used exclusively by the processor for both encryption and decryption (Fig 5; col 4, lines 27-29; and col 8, lines 18-18). *A DES secret key is operable to be exclusively used by the processor for both encryption and decryption.*
2. A cryptographic engine for performing the key-based cryptographic process internally within the processor (Fig 5, DES engine 21), wherein the cryptographic engine is configured to access the digital secret (col 8, lines 18-22 and Fig 5).

Easter does not explicitly disclose wherein the digital secret is stored only within the processor and internal memory coupled to the cryptographic engine and configured to support the key-based cryptographic process, wherein the internal memory is further configured to store data associated with the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein the data is accessible only within the processor.

However, Easter discloses storing a key only within an integrated circuit (col 5, lines 6-11 and col 6, lines 14-19). Further, Hashimoto discloses a single package microprocessor with a unique digital secret stored only within the processor (col 6, lines 45-48). Additionally, Hashimoto an internal memory (i.e. Fig 3, processor cache 114) coupled to the cryptographic engine (Fig 3) and configured to support the key-based cryptographic process, wherein the internal memory is further configured to store data associated with the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein the data is accessible only within the processor (col 7, lines 32-42; col 12, lines 5-41; and col 29, lines 35-56).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Easter's invention using Hashimoto's teachings according to the limitations recited in claim 1 by incorporating the cryptographic IC chip disclosed by Easter as part of a single microprocessor package as taught by Hashimoto and by utilizing a cryptographic engine such as engine 113 seen in Figure 3 of Hashimoto having an internal memory as disclosed by Hashimoto in the portions cited above. One skilled would have been motivated to incorporate Easter's IC circuit into a single microprocessor package as taught by Hashimoto because Easter's IC chip is meant to be incorporated as part of further circuitry (Easter: col 6, lines 14-15). One skilled would have been motivated to have an internal memory as disclosed by Hashimoto because it would ensure that secrets that belong to applications executing on a processor stays a secret (Hashimoto: col 5, lines 11-20 and col 6, lines 19-28).

**Claim 10:**

Easter discloses:

1. A secure cryptographic unit (Fig 5, item 53), the cryptographic unit comprising:
    a. A cryptographic engine configured to perform a key-based cryptographic process (Fig 5, items 57 and 21).
    b. A digital secret exclusively accessible to the cryptographic engine, wherein the digital secret includes a secret key used in the key-based cryptographic process, and wherein the secret key is configured to be used exclusively by the processor for both encryption and decryption (col 4, lines 28-29 and col 8, lines 10-22).

Easter does not explicitly disclose wherein the cryptographic unit is configured to internally provide secure cryptographic capabilities as a functional unit within the processor. Easter also does not explicitly disclose internal memory coupled to the cryptographic engine and configured to support the key-based cryptographic process, wherein the internal memory is further configured to store data associated with the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein the data is accessible only within the processor.

However, Easter discloses that his secure cryptographic unit is meant to be incorporated into further circuitry (col 6, lines 15-16). Easter discloses storing a key only within an integrated circuit (col 5, lines 6-11 and col 6, lines 14-19). Further, Hashimoto discloses a single package microprocessor with a unique digital secret stored only within the processor (col 6, lines 45-48). Additionally, Hashimoto an internal memory (i.e. Fig 3, processor cache 114) coupled to the cryptographic engine (Fig 3) and configured to support the key-based cryptographic process, wherein the internal memory is further configured to store data associated with the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein the data is accessible only within the processor (col 7, lines 32-42; col 12, lines 5-41; and col 29, lines 35-56).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Easter's invention using Hashimoto's teachings according to the limitations recited in claim 10. One skilled would have been motivated to do so for the same reasons discussed in claim 1.

**Claim 21:**

Easter discloses:

1. A secure hardware environment configured to provide core processing functionality (Fig 5, item 53), wherein the secure hardware environment comprises:
    a. A secure cryptography unit (Fig 5, item 21) configured to provide secure cryptographic capabilities as a functional unit within the secure hardware

environment (Fig 5), wherein the secure cryptography unit is configured to facilitate performance of a key-based cryptographic process, wherein the key-based cryptographic process includes encryption using a digital secret and decryption using the digital secret, and wherein the key-based cryptographic process further includes generating data (col 4, lines 28-29 and col 8, lines 10-22).

Easter does not explicitly disclose the key-based cryptographic process is performed exclusively by the processor and wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein the data is accessible only within the processor.

However, Easter discloses that his secure cryptographic unit is meant to be incorporated into circuitry (col 6, lines 15-16). Easter discloses storing a key only within an integrated circuit (col 5, lines 6-11 and col 6, lines 14-19). Further, Hashimoto discloses a single package microprocessor with a unique digital secret stored only within the processor (col 6, lines 45-48). Additionally, Hashimoto an internal memory (i.e. Fig 3, processor cache 114) coupled to the cryptographic engine (Fig 3) and configured to support the key-based cryptographic process, wherein the internal memory is further configured to store data associated with the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process, and wherein the data is accessible only within the processor (col 7, lines 32-42; col 12, lines 5-41; and col 29, lines 35-56).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Easter's invention using Hashimoto's teachings according to the limitations recited in claim 21. One skilled would have been motivated to do so for the same reasons discussed in claim 1.

**Claim 2:**

Hashimoto further discloses an internal bus configured to facilitate secure communication between the cryptographic engine, the digital secret, and the internal memory within said processor (Figures 1 and 3 and col 5, lines 57-67).

**Claim 3:**

Hashimoto further discloses wherein the digital secret is securely confined within the processor (col 6, lines 45-48).

**Claim 5:**

Easter discloses wherein the data includes intermediate data generated by the key-based cryptographic process (col 8, lines 10-12 and 37-40). *The DES algorithm generates intermediate data and is a key-based cryptographic process.*

**Claim 6:**

As per the limitation that the processor of claim 1 further comprises a cryptographic unit including a functional unit within the processor for securely executing the key-based cryptographic process internally within the processor, wherein the cryptographic unit comprises: the digital secret; the cryptographic engine; and the internal memory, it is obvious to the combination invention of Easter and Hashimoto. Note that as discussed in claim 1, the digital secret; the cryptographic engine; and the internal memory are contained in Easter's integrated circuit 53 (Fig 5), which is meant for incorporation into circuitry (col 6, lines 14-15). If one were to incorporate integrated circuit 53 into Hashimoto's processor as intended by Easter, one would end up with a processor as recited in claim 6. Integrated circuitry 53 can be considered the recited cryptographic unit. Note also that making things separate or integral is obvious (see MPEP 2144.04(V)(B)).

**Claims 7 and 11:**

Easter further discloses wherein the key-based cryptographic process includes: a key based encryption process; and a key-based decryption process (col 4, lines 27-29).

**Claims 9 and 14:**

Easter does not explicitly disclose wherein the digital secret is unique to the processor and is permanently and physically manifested within the processor. However, official notice is taken that using a key unique to a processor was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to utilize a digital secret that was unique to the processor because a DES key is meant to be secret and use of a unique key would prevent accidental access to the software being secured by Easter and Hashimoto's secure processor.

Further, Easter discloses that it was known to permanently and physically manifest a key within a processor (col 2, lines 44-46; col 5, lines 6-11; and col 8, lines 29-31). Storing of a key via a fuse array would permanently and physically manifest a key within the processor. At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Easter and Hashimoto's combination invention such that the DES key was permanently and physically manifest a key within the processor. The rationale for why it is obvious is that the simple substitution of a key which is not permanently and physically manifested in the processor for one that is would do no more than yield a predictable result. One skilled would have been motivated to do so because it would ensure the secrecy of the key (col 8, lines 29-31).

**Claim 15:**

Easter does not explicitly disclose wherein the digital secret comprises a plurality of fusible links configured to manifest the digital secret by permanently setting a binary state in each of the plurality of fusible links. However, Easter discloses that it was known in the art to use a plurality of fusible links configured to manifest a key by permanently setting a binary state in each of the plurality of fusible links (col 5, lines 10-11 and 26-47 and col 8, lines 29-31).

At the time applicant's invention was made, it would have been obvious to further modify Easter and Hashimoto's combination invention according to the limitations recited in claim 15 by programming a fuse array to store the DES key. The rationale for why it is obvious is that use of a fuse array to store the DES key instead of key array 25 is nothing more that the simple substitution of one known element for another to obtain the predictable result of a DES key stored in a fuse array. One skilled would have been motivated to do so because it would ensure the secrecy of the key (col 8, lines 29-31).

**Claims 18 and 25:**

Hashimoto further discloses wherein the secure cryptographic unit is a fully integrated circuit within the processor (Fig 3).

**Claim 19:**

Hashimoto further discloses wherein the digital secret and the internal memory are fully integrated with the cryptography engine to facilitate communication without use of a bus (Fig 3 and col 5, lines 56-67).

Note that the above limitation is interpreted as best understood from what is disclosed in the specification. The examiner assumes that “without use of a bus” refers to an external bus and does not refer to internal buses since one skilled in the art would recognize that any type of circuit would have some form of busses, thus the total absence of a bus in a circuit or processor is impossible.

**Claim 20:**

Easter does not explicitly disclose wherein the key-based cryptography process comprises a Triple Data Encryption Algorithm (TDEA or Triple DES) cryptographic process. However, official notice is taken that Triple DES was a well known cryptographic process at the time applicant’s invention was made. It would have been obvious to one skilled in the art to modify Easter’s invention such that the key-based cryptography process comprises Triple DES cryptographic process. One skilled would have done so because Triple DES is more secure than DES. Further, it would have been obvious to do so because the substitution of a Triple DES engine for a DES engine would do no more than yield a predictable result.

Claim 4 is rejected under 35 U.S.C. 103(a) as obvious over Easter et al (US 5,563,950) in view of Hashimoto et al (US 6,983,374) in further view of Galasso (US 6,598,165) and Moyer et al (US 2004/0243823).

**Claim 4:**

Easter does not explicitly disclose wherein the internal memory includes microcode for implementing the key based-based cryptographic process on the data within the processor, and wherein the internal memory is configured to perform state tracking associated with the key-based cryptographic process.

However, Galasso discloses a key-based cryptographic process performed on data within a processor which utilizes microcode contained in an internal memory (col 3, lines 1-20). At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Easter and Hashimoto's combination invention such that the internal memory comprises microcode for implementing the key based-based cryptographic process on data within the processor. The rationale for why this is obvious is that the simple substitution of the DES engine disclosed by Easter with a software based DES engine disclosed by Galasso, which requires the internal memory to comprise microcode for implementing the DES algorithm is nothing more than simple substitution of one known element for another to obtain predictable results.

Further, Moyer discloses internal memory operable to perform state tracking associated with a data processing system (paragraphs 12 and 14). Moyer's invention tracks the state of a data processing system to determine when errors or access violations may occur (paragraph 4). At the time applicant's invention was made, it would have been obvious to further modify the combination invention of Easter, Hashimoto, and Galasso such that the internal memory is operable to perform state tracking associated with the key-based cryptographic process. One skilled would have been motivated to do so because it would improve the security (Moyer: paragraph 38) of the secure processor having the software DES engine by catching errors and access violations. Note that the DES engine is a data processing system.

Claims 8, 13, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Easter et al (US 5,563,950) in view of Hashimoto et al (US 6,983,374) in further view of Fahrny (US 2004/0098591).

**Claims 8, 13, and 22:**

Easter further discloses a secure hardware environment providing core processing functionality (Fig 5).

Easter does not explicitly disclose secure software environment coupled to the secure hardware environment, wherein the secure software environment is configured to generate executable instructions that are sent to the secure hardware environment for processing, wherein the secure hardware environment in combination with the secure software environment is configured to provide processor capability, and wherein the secure hardware environment is accessible only through the secure software environment.

However, Fahrny discloses a secure software environment coupled to a secure hardware environment (paragraphs 10 and 26), the secure software environment generating executable instructions that are sent to the secure hardware environment for processing (Fig 1 and paragraphs 26-28), the secure hardware environment in combination with the secure software environment providing processor capability, and wherein the secure hardware environment is accessible only through the secure software environment (Fig 1, item 16 and paragraphs 28 and 31).

Note in the cited section of Fahrny that a secure hardware (Fig 1, item 16) authenticates software objects, including a trusted operating system at initialization. Access to any items in the secure hardware has to be done via an authenticated software object, i.e. trusted OS. The combination of authenticated software objects, i.e. secure software environment, along with the secure hardware (Fig 1, item 16) provides processor capability.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Easter and Hashimoto's combination invention according to the limitations recited in claim 8 in light of Fahrny's teachings. One skilled would have been motivated to do so because Fahrny's teachings would further protect data within a secure hardware, i.e. Easter and Hashimoto's secure processor, by authenticating software objects prior to allowing the software object access to any data in the secure hardware (Fahrny: paragraph 10). This would further ensure that unauthorized users could not access the software encrypted software or DES key illegally.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Easter et al (US 5,563,950) in view of Hashimoto et al (US 6,983,374) in further view of Cmelik et al (US 6,031,992).

**Claim 12:**

Easter does not explicitly disclose wherein the processor comprises a very long instruction word processor (VLIW) processor. However, Cmelik discloses wherein a processor comprises a very long instruction word processor (VLIW) processor (col 8, lines 51-65). At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Easter's invention according to the limitations recited in claim 12 in light of Cmelik's teachings. One skilled would have been motivated to dos o because use of a VLIW processor would increase the speed of processor execution (Cmelik: col 9, lines 51-65).

Claims 23, 24, and 26 are rejected under 35 U.S.C. 103(a) as obvious over Easter et al (US 5,563,950) in view of Hashimoto et al (US 6,983,374) in further view of Moyer et al (US 2004/0243823)

**Claim 23:**

Easter further discloses wherein the secure cryptography unit includes:

1. A cryptography engine configured to perform the key based cryptographic process (Fig 5, DES engine 21).
2. The digital secret accessible exclusively to the cryptography engine , wherein the digital secret includes a secret key used in the key-based cryptographic process (col 4, lines 28-29 and col 8, lines 10-22).
3. Internal memory coupled to the cryptography engine, wherein the internal memory is configured to support the key-based cryptographic process (Fig 5, items 25 and 37).

Easter does not explicitly disclose the internal memory is further configured to perform state tracking associated with the key-based cryptographic process. However, software based DES engine were well known in the art. Further, Moyer discloses internal memory operable to perform state tracking associated with a data processing system (paragraphs 12 and 14). Moyer's invention tracks the state of a data processing system to determine when errors or access violations may occur (paragraph 4). At the time applicant's invention was made, it would have been obvious to further modify the combination invention of Easter and Hashimoto such that a software DES engine was used and the internal memory is operable to perform state tracking associated with the key-based cryptographic process. One skilled would have been motivated to use a software DES engine because use of a software or hardware DES engine is an obvious design choice. One skilled would have been motivated to incorporate Moyer's teachings in the manner discussed because it would improve the security (Moyer: paragraph 38) of the secure processor having the software DES engine by catching errors and access violations. Note that the DES engine is a data processing system.

**Claim 24:**

Easter and Hashimoto further discloses wherein the internal memory is operable to securely store the data (Hashimoto: col 7, lines 32-42; col 12, lines 5-41; and col 29, lines 35-56), and wherein the data comprises intermediate data generated by the key-based cryptographic process (Easter: Fig 2 and col 8, lines 10-12).

**Claim 26:**

Claim 26 recites a further limitation substantially similar to what is recited in claim 19 and is rejected for similar reasons.

## ***Allowable Subject Matter***

Claims 16-17 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

## ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Examiner, Art Unit 2435